PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-109439
(43)Date of publication of application : 12.04.2002

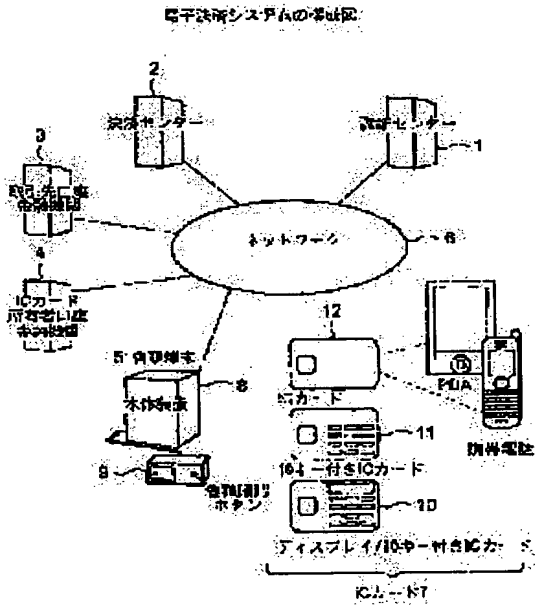
(51)Int.Cl. G06F 17/60
B42D 15/10
G06F 15/00
G06K 17/00
G06K 19/077
G06K 19/07

(21)Application number : 2000-301281
(22)Date of filing : 29.09.2000

(71)Applicant : RICOH CO LTD
(72)Inventor : YANO TAKASHI

(54) ELECTRONIC ACCOUNT SETTLEMENT SYSTEM, IC CARD, ELECTRONIC SETTLEMENT EQUIPMENT AND RECORDING MEDIUM IN WHICH THE PROGRAM IS RECORDED

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic account settlement system which improves the security by preventing an illegal recording of a password or information on a living body and also by preventing an illegal settlement.
SOLUTION: This system is an electronic account settlement system which performs an electronic settlement using an IC card, that is, it performs a transaction of an electronic settlement using personal information which is input in the IC card by a user beforehand and information about transaction amount, etc. The personal information consists of a password and the information on a living body, and by which a personal certification is performed. The information about transaction amount, etc., consists of a maximum transaction amount limit and a transaction amount, and the transaction by an false transaction amount is prevented by transmitting from the IC card the maximum transaction amount limit and the transaction amount to the electronic settlement equipment.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－109439
（P2002－109439A）
(43)公開日　平成14年４月12日(2002.4.12)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　17/60	４１４	Ｇ０６Ｆ　17/60	４１４	２Ｃ００５
	２４２		２４２	５Ｂ０３５
	５１０		５１０	５Ｂ０４９
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	５Ｂ０５５
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｂ０５８

審査請求　未請求　請求項の数25　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2000－301281(P2000－301281)

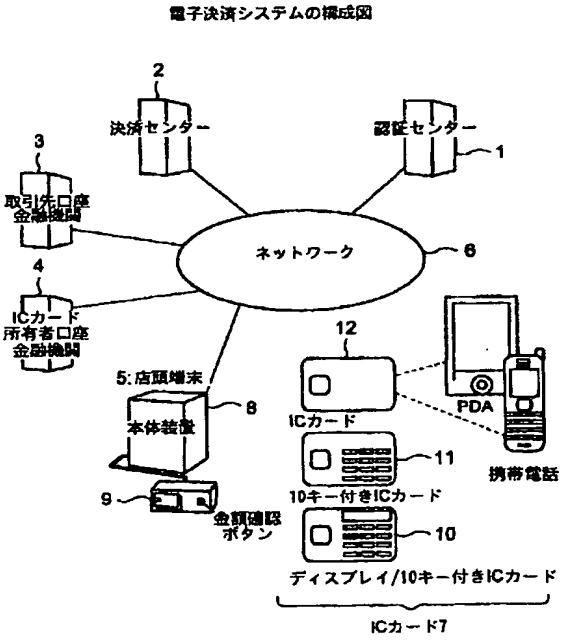
(22)出願日　平成12年９月29日(2000.9.29)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　矢野　隆志
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　電子決済システム、ＩＣカード、決済装置、及びそのプログラムを記録した記録媒体

(57)【要約】
【課題】　パスワードや生体情報の不正な記録を防止し、不正な決済を防止することによりセキュリティを向上させた電子決済システムを提供することを目的とする。
【解決手段】ＩＣカードを用いて電子決済を行う電子決済システムであり、利用者によって予めＩＣカードに入力された個人情報や取引額等の情報を用いて電子決済における処理を行う。個人情報はパスワードや生体情報であり、これにより個人認証を行う。取引額等の情報は取引限度額や取引額であり、ＩＣカードから取引限度額や取引額を決済装置に送信することにより、不正な取引額による取引が行われることを防止する。



【特許請求の範囲】

【請求項１】　ＩＣカードを用いて電子決済を行う電子決済システムであって、
利用者によって予めＩＣカードに入力された情報を用いて電子決済における処理を行うことを特徴とする電子決済システム。

【請求項２】　前記情報は個人情報であり、該個人情報を用いてＩＣカードの認証処理を行う請求項１に記載の電子決済システム。

【請求項３】　前記電子決済システムは認証装置を有し、前記認証処理において、
前記ＩＣカードは属性情報を認証装置に送信し、
該認証装置は認証信号を該ＩＣカードに送信し、
該ＩＣカードは該認証信号と前記個人情報を含む情報に演算を施し、認証応答信号を生成して該認証装置に送信し、
該認証装置が該認証応答信号を用いて認証を行う請求項２に記載の電子決済システム。

【請求項４】　前記ＩＣカードに入力された個人情報を一回の取引における使用に限定する請求項２又は３に記載の電子決済システム。

【請求項５】　前記個人情報はパスワード又は生体情報である請求項２ないし４のうちいずれか１項に記載の電子決済システム。

【請求項６】　前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する請求項１に記載の電子決済システム。

【請求項７】　前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引限度額であり、
前記ＩＣカードは取引限度額を決済装置に送信し、
決済装置は、該取引限度額を受信し、店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信し、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する請求項６に記載の電子決済システム。

【請求項８】　前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引額であり、
前記ＩＣカードは取引額を決済装置に送信し、
決済装置は、該取引額を受信し、前記店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信し、ＩＣカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する請求項６に記載の電子決済システム。

【請求項９】　前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引限度額であり、前記電子決済システムが電子マネー型である場合において、
前記店頭端末に装着されたＩＣカードに、該店頭端末から取引限度額を超える取引要求がある場合に該ＩＣカードは該取引要求を拒絶する請求項６に記載の電子決済システム。

【請求項１０】　前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引額であり、前記電子決済システムが電子マネー型である場合において、
前記店頭端末に装着されたＩＣカードに、前記店頭端末から前記取引額と異なる取引額による取引要求がある場合に該ＩＣカードは該取引要求を拒絶する請求項６に記載の電子決済システム。

【請求項１１】　店頭端末を有する電子決済システムで使用するＩＣカードであって、
テンキーと、
テンキーを用いて入力された情報を保持する手段と、
該情報を店頭端末に送信する手段とを有することを特徴とするＩＣカード。

【請求項１２】　テンキーを用いて入力された情報を表示するディスプレイを更に有する請求項１１に記載のＩＣカード。

【請求項１３】　入力された情報を所定の処理の後に削除する手段を更に有する請求項１１に記載のＩＣカード。

【請求項１４】　消費税を算出するためのキーを更に有する請求項１２又は１３に記載のＩＣカード。

【請求項１５】　前記電子決済システムが電子マネー型である場合において、
前記情報として取引限度額を保持する手段と、
店頭端末から取引限度額を超える取引要求がある場合に該取引要求を拒絶する手段とを更に有する請求項１１に記載のＩＣカード。

【請求項１６】　前記電子決済システムが電子マネー型である場合において、
前記情報として取引額を保持する手段と、
店頭端末から前記取引額と異なる取引額による取引要求がある場合に該取引要求を拒絶する手段とを更に有する請求項１１に記載のＩＣカード。

【請求項１７】　ＩＣカードを用いて電子決済を行う電子決済システムにおける決済装置であって、
利用者によって予めＩＣカードに入力された情報を受信し、その情報を用いて電子決済における処理を行うことを特徴とする決済装置。

【請求項１８】　前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手段を有する請求項１７に記載の決済装置。

【請求項１９】　前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、
前記ＩＣカードから取引限度額を受信する手段と、
店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手段と、
該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手段とを有する請求項１８に記載の決済装置。

【請求項２０】　前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、
前記ＩＣカードから取引額を受信する手段と、
店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手段と、
ＩＣカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手段とを有する請求項１８に記載の決済装置。
【請求項２１】　ＩＣカードを用いて電子決済を行う電子決済システムにおける決済処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
利用者によって予めＩＣカードに入力された情報を受信し、その情報を用いて電子決済における処理手順をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２２】　前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手順を有する請求項２１に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２３】　前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、
前記ＩＣカードから取引限度額を受信する手順と、
店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手順と、
該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手順とを有する請求項２２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２４】　前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、
前記ＩＣカードから取引額を受信する手順と、
店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手順と、
ＩＣカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手順とを有する請求項２２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２５】　ＩＣカードを用いて電子決済を行う電子決済システムであって、
ＩＣカードに所定の情報を入力する第１の端末と、
前記ＩＣカードから所定の情報を取り出して操作部から入力された取引の情報に関する情報とともに送信する第２の端末とを有する電子決済システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、商取引によって発生する購入代金、使用料等の決済をネットワークやＩＣカードを利用して行う電子決済に関する。
【０００２】
【従来の技術】電子決済にはネットワーク型電子決済とカード型電子決済がある。ネットワーク型電子決済は仮想世界の商取引に使用され、電子財布と呼ばれる概念のソフトウェアで貨幣価値の保存、転送を行う。カード型電子決済は実世界の商取引に使用することができ、メモリーで貨幣価値の保存を行う。本発明はこれらのうちのカード型電子決済、特にＩＣカードを利用したカード型電子決済を対象としており、以下、カード型電子決済の従来技術について説明する。
【０００３】カード型電子決済には、クレジットカード型、電子マネー型、キャッシュカード型の３種類の方式がある。
【０００４】クレジットカード型におけるカードはクレジット会社が発行し、決済は２５－５５日後に所有者の銀行口座から引き落とされ、取引先の銀行口座に振り込まれることにより行われる。クレジットカード型では本人認証にサインを用いるので支払に手間がかかり、使用は一般的に高額の取引に限定される。
【０００５】電子マネー型には例えばビザ・キャッシュ、モンデックス、プロトン、スーパーキャッシュ等があり、電子マネーは主に金融機関が発行する。電子マネー型で使用するカードが記憶しているのは貨幣価値情報であり、カードを使用する際には本人確認の必要はなく、他人の使用もできる。決済は貨幣価値情報の転送でリアルタイムに行われ、主に少額取引に用いられる。
【０００６】電子マネー型では、店頭端末における目視による金額確認と確認ボタンの操作(決済がその場で完結し証拠が残らないため)が必要であること等のため、あまり普及していない。
【０００７】キャッシュカード型には例えばデビットカードがあり、カードは主に金融機関が発行する。本人確認は所有者のパスワード(例えば銀行口座暗証番号)で行われ、決済はリアルタイムに所有者の銀行口座から引き落とされ取引先の銀行口座に振り込まれる。預金残高以上の取引はできず、主に少額取引に用いられる。
【０００８】キャッシュカード型における本人確認には所有者のパスワード(銀行口座暗証番号)が用いられ、これが盗まれると所有者の銀行口座の預金が危険にさらされると言う問題点がある。
【０００９】さて、上記の電子決済システムには利用者が用いるカードとして磁気カード等やＩＣカードが用いられる。磁気カード等を用いた場合にはユーザ認証をユーザＩＤ(カードＩＤ)とパスワード(ユーザが入力するパスワード)によって行っており、ユーザＩＤとパスワードが容易に傍受されるという問題がある。一方、ＩＣカードは磁気カード等と比較して情報の読みだしが困難であり、偽造も困難である。また、暗号処理を行うことにより、パスワードによるユーザ認証を暗号アルゴリズムを用いて行い、更に、耐タンパー性を持たせる(漏洩

電磁波のシールド等)ことにより、磁気カード等と比較してユーザ認証能力と偽造防止能力が高い。

【００１０】

【発明が解決しようとする課題】しかしながら、ＩＣカードを用いた電子決済システムでも、利用者はＩＣカードの所有者であることを証明するために店頭端末にパスワードを入力することが必要である。この時、パスワードを第三者に見られる可能性があり、また、店頭端末に直接パスワードを入力するために悪意によって改造された店頭端末によってパスワードの記録を取られる可能性がある。従って、パスワードが盗まれる可能性があるという問題点がある。パスワードが盗まれると不正な架空の決済が行われる可能性がある。

【００１１】指紋等の生体情報の認識技術であるバイオメトリックスもユーザ認証に使用されてきているが、この場合にも、ＩＣカードの所有者であることの証明に店頭端末で生体情報を読み取る必要があり、悪意によって改造された店頭端末によって生体情報を記録される可能性がある。

【００１２】また、上記従来の技術によると、ＩＣカード所有者に提供する情報と異なる情報を決済センターに提供することにより不正な決済(異なる金額の決済)が行われる可能性があるという問題点がある。これはパスワードや生体情報が盗まれなくても起こりうる。

【００１３】更に、店頭端末へのパスワード入力に時間がかかり、営業効率に影響を及ぼすという問題がある。また、クレジットカード型ではサインの処理に時間を要し、電子マネー型では店頭端末へのパスワード入力、金額確認ボタンの操作に時間を要し、キャッシュカード型では金額確認ボタンの操作に時間を要するという問題点がある。

【００１４】本発明は上記の点に鑑みてなされたものであり、パスワードや生体情報の不正な記録を防止し、不正な決済を防止することによりセキュリティを向上させ、更に店頭端末における操作時間を短縮させた電子決済システムを提供することを目的とする。

【００１５】

【課題を解決するための手段】上記の目的を達成するために本発明は次のように構成することができる。

【００１６】請求項１に記載の発明は、ＩＣカードを用いて電子決済を行う電子決済システムであって、利用者によって予めＩＣカードに入力された情報を用いて電子決済における処理を行う。

【００１７】本発明によれば、予めＩＣカードに入力された情報を用いるので、改造された店頭端末等により入力情報が記録されるという問題点を解消でき、セキュリティーを向上させることができる。また、改造された店頭端末等の不正により実際と異なる取引額による決済が行われることを防止することが可能となる。

【００１８】請求項２に記載の発明は、請求項１の記載において、前記情報は個人情報であり、該個人情報を用いてＩＣカードの認証処理を行うようにする。

【００１９】本発明によれば、特に、パスワード等の個人情報が改造された店頭端末等により記録されるという問題点を解消できる。

【００２０】請求項３に記載の発明は、請求項２の記載において、前記電子決済システムは認証装置を有し、前記認証処理において、前記ＩＣカードは属性情報を認証装置に送信し、該認証装置は認証信号を該ＩＣカードに送信し、該ＩＣカードは該認証信号と前記個人情報を含む情報に演算を施し、認証応答信号を生成して該認証装置に送信し、該認証装置が該認証応答信号を用いて認証を行う。これにより、ＩＣカード利用者の認証を、個人情報が傍受されることなく行うことができる。

【００２１】請求項４に記載の発明は、請求項２又は３の記載において、前記ＩＣカードに入力された個人情報を一回の取引における使用に限定する。

【００２２】本発明により、個人情報が盗まれる危険を防止することができる。

【００２３】請求項５に記載の発明は、請求項２ないし４のうちいずれか１項の記載において、前記個人情報はパスワード又は生体情報であるとする。パスワード又は生体情報を用いることにより、個人認証を行うことができる。

【００２４】請求項６に記載の発明は、請求項１の記載において、前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する。

【００２５】本発明によれば、改造された店頭端末等を用いた不正により実際と異なる取引額による決済が行われることを防止することが可能となる。

【００２６】請求項７に記載の発明は、請求項６の記載において、前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引限度額であり、前記ＩＣカードは取引限度額を決済装置に送信し、決済装置は、該取引限度額を受信し、店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信し、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する。

【００２７】本発明によれば、取引額が取引限度額を超えることがなくなり、不正や過誤により過大な取引額による決済が行われることを防止できる。

【００２８】請求項８に記載の発明は、請求項６の記載において、前記電子決済システムは店頭端末と決済装置を有し、前記取引の額に関する情報は取引額であり、前記ＩＣカードは取引額を決済装置に送信し、決済装置は、該取引額を受信し、前記店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信し、ＩＣカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒

絶する。

【００２９】本発明によれば、不正により実際と異なる取引額による取引要求がなされた場合でも、その取引要求は拒絶されるため、取引の安全を確保でき、セキュリティーを高めることができる。また、店頭端末における金額確認が不要となるため、操作が容易になり、利用者の利便性が向上するとともに、店における業務効率も向上する。

【００３０】請求項９に記載の発明は、請求項６の記載において、前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引限度額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたＩＣカードに、該店頭端末から取引限度額を超える取引要求がある場合に該ＩＣカードは該取引要求を拒絶する。

【００３１】本発明によれば、請求項７と同様の作用効果を得ることができる。

【００３２】請求項１０に記載の発明は、請求項６の記載において、前記電子決済システムは店頭端末を有し、前記取引に関する情報は取引額であり、前記電子決済システムが電子マネー型である場合において、前記店頭端末に装着されたＩＣカードに、前記店頭端末から前記取引額と異なる取引額による取引要求がある場合に該ＩＣカードは該取引要求を拒絶する。

【００３３】本発明によれば、請求項８と同様の作用効果を得ることができる。

【００３４】請求項１１に記載の発明は、店頭端末を有する電子決済システムで使用するＩＣカードであって、テンキーと、テンキーを用いて入力された情報を保持する手段と、該情報を店頭端末に送信する手段とを有する。

【００３５】本発明によれば、上記電子決済システムでの使用に適したＩＣカードを提供することができる。

【００３６】請求項１２に記載の発明は、請求項１１の記載において、テンキーを用いて入力された情報を表示するディスプレイを更に有する。これにより入力を確認することができる。

【００３７】請求項１３に記載の発明は、請求項１１の記載において、入力された情報を所定の処理の後に削除する手段を更に有する。本発明によれば、処理の度に新たに情報を入力することとなるので、セキュリティーを高めることができる。

【００３８】請求項１４に記載の発明は、請求項１２又は１３の記載において、消費税を算出するためのキーを更に有する。これにより、正確かつ迅速に取引額を入力することができる。

【００３９】請求項１５に記載の発明は、請求項１１の記載において、前記電子決済システムが電子マネー型である場合において、前記情報として取引限度額を保持する手段と、店頭端末から取引限度額を超える取引要求がある場合に該取引要求を拒絶する手段とを更に有する。本発明によれば、請求項９の電子決済システムでの使用に適したＩＣカードを提供できる。

【００４０】請求項１６に記載の発明は、請求項１１の記載において、前記電子決済システムが電子マネー型である場合において、前記情報として取引額を保持する手段と、店頭端末から前記取引額と異なる取引額による取引要求がある場合に該取引要求を拒絶する手段とを更に有する。本発明によれば、請求項１０の電子決済システムでの使用に適したＩＣカードを提供できる。

【００４１】請求項１７に記載の発明は、ＩＣカードを用いて電子決済を行う電子決済システムにおける決済装置であって、利用者によって予めＩＣカードに入力された情報を受信し、その情報を用いて電子決済における処理を行う。

【００４２】本発明によれば、請求項１と実質的に同様の作用効果を奏する。

【００４３】請求項１８に記載の発明は、請求項１７の記載において、前記情報は取引の額に関する情報であり、該取引の額に関する情報を用いて決済処理を行うか否かを判断する手段を有する。

【００４４】本発明によれば、請求項６と実質的に同様の作用効果を奏する。

【００４５】請求項１９に記載の発明は、請求項１８の記載において、前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引限度額であり、前記ＩＣカードから取引限度額を受信する手段と、店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手段と、該取引額が前記取引限度額を超える場合に該取引要求を拒絶する手段とを有する。

【００４６】本発明によれば、請求項７と実質的に同様の作用効果を奏する。

【００４７】請求項２０に記載の発明は、請求項１８の記載において、前記電子決済システムは店頭端末を有し、前記取引の額に関する情報は取引額であり、前記ＩＣカードから取引額を受信する手段と、店頭端末からＩＣカードの利用者の取引額を含む取引要求を受信する手段と、ＩＣカードから受信した取引額と前記店頭端末から受信した取引額とを比較し、それらが一致しない場合には該取引要求を拒絶する手段とを有する。

【００４８】本発明によれば、請求項８と実質的に同様の作用効果を奏する。

【００４９】請求項２１～請求項２４に記載の発明によれば、請求項１７～２０の決済装置の処理を行うことに適したプログラムを記録した記録媒体を提供することができる。

【００５０】また、請求項２５に記載の発明は、ＩＣカードを用いて電子決済を行う電子決済システムであって、ＩＣカードに所定の情報を入力する第１の端末と、前記ＩＣカードから所定の情報を取り出して操作部から

入力された取引の情報に関する情報とともに送信する第２の端末とを有する。

【００５１】本発明によれば、請求項１に記載の発明と実質的に同様の作用効果を奏する。

【００５２】

【発明の実施の形態】［第１の実施例］図１に本発明の実施例における電子決済システムの構成を示す。同図に示すように、本電子決済システムは、認証センター１（認証装置ともいう）、決済センター２（決済装置ともいう）、取引先口座金融機関３、ＩＣカード所有者口座金融機関４、店頭端末５を有し、それぞれがネットワーク６に接続される。また、ＩＣカード７は、店頭端末５に装着されることによりネットワーク６を介してデータを送受信できる。

【００５３】認証センター１はＩＣカードの認証を行い、決済センター２が決済処理を行う。取引先口座金融機関３は、取引相手の口座を持つ金融機関であり、ある物を購入した場合の代金はこの口座に振り込まれる。ＩＣカード所有者口座金融機関４は、ＩＣカード所有者の口座を持つ金融機関であり、購入代金がここから引き落としされる。

【００５４】認証センター１と決済センター２は、クレジットカード型ではクレジット会社にある。

【００５５】また、一般的な電子マネー型ではパスワード認証を行わないので認証センター１はないが、パスワード認証を行う電子マネー型では認証センターが必要であり、本実施例においてはパスワード認証を行うものとして説明する。電子マネー型における決済センター２は銀行等のカード発行金融機関にあり、ＩＣカード所有者はカード発行金融機関に口座を作る。

【００５６】キャッシュカード型では認証センター１と決済センター２共に銀行等のカード発行金融機関にあり、この場合もＩＣカード所有者はカード発行金融機関に口座を作る。

【００５７】認証センター１と決済センター２はそれぞれコンピュータを用いて実現することができる。図２に決済センター２の構成例を示す。なお、認証センター１も図２に示す構成と同様の構成をとることができる。図２に示すように、決済センター２は、ＣＰＵ（中央処理装置）１０１、メモリ１０２、入力装置１０３、表示装置１０４、ＣＤ－ＲＯＭドライブ１０５、ハードディスク１０６、通信処理装置１０７を有する。ＣＰＵ１０１は装置の全体を制御する。メモリ１０２はＣＰＵ１０１で処理するデータやプログラムを保持する。入力装置１０３はキーボードやマウス等のデータを入力するための装置である。表示装置１０４はディスプレイ等の装置である。ＣＤ－ＲＯＭドライブ１０５はＣＤ－ＲＯＭ等を駆動し、データやプログラムの読み出しを行う。ハードディスク１０６には、プログラムや、本発明の処理に関わるデータが格納される。通信処理装置１０７によりデータをネットワークを介して送受信する。また、データの保存等のためにＭＴ装置を接続してもよい。本発明の電子決済処理を実行するプログラムは、コンピュータに予めインストールされていてもよいし、例えばＣＤ－ＲＯＭに格納され、ＣＤ－ＲＯＭドライブ１０５を介してハードディスク１０６にロードするようにしてもよい。プログラムが起動されると、所定のプログラム部分がメモリ１０２に展開され、処理が実行される。

【００５８】なお、認証センター１と決済センター２を統合することも可能である。また、認証センター１と決済センター２をカード発行金融機関から独立させ、電子マネー/キャッシュカードの運営グループの運営とすることもできる。

【００５９】取引先口座金融機関３、ＩＣカード所有者口座金融機関４の構成及び動作は従来と同様である。

【００６０】店頭端末５は、本体装置８とＩＣカードを装着するリーダーライター９を有する。本体装置８は例えばコンピュータを用いて実現できる。また、本体装置８をＰＯＳ端末としてもよい。また、本体装置とリーダーライターを一体として構成することもできる。

【００６１】ネットワーク６としては、例えばインターネット、回線交換ネットワーク、専用回線を使用することができる。

【００６２】図１に示すように、ＩＣカードとしては、ディスプレイとテンキー付きＩＣカード１０、テンキー付きＩＣカード１１、ＰＤＡや携帯電話とのインターフェースを有するＩＣカード１２を使用できる。

【００６３】ディスプレイとテンキー付きＩＣカード１０の構成を図３に示す。

【００６４】ディスプレイとテンキー付きＩＣカード１０は、店頭端末等から信号や電力を受信するアンテナ２１、信号の送受信を行うトランシーバ２２、処理・制御を行うＣＰＵ２３、入力データ等を保持するＲＡＭ２４、プログラムと秘密鍵を記憶するＥＰＲＯＭ２５（一般的にはフラッシュメモリーが用いられる）、情報を入力するためのテンキー２６、テンキーからの入力を符号化するテンキーエンコーダ２７、情報を表示するＬＣＤ（liquid crystal display）２８、ＬＣＤを制御するディスプレイドライバ２９、アンテナや電池内蔵ウォレットから受信した電力を受電する受電器３０、電力を蓄えるキャパシタ３１、受電器３０からの電力とキャパシタ３１を切替えるための切替器３２を有する。

【００６５】上記の構成において、ＬＣＤ２８、ディスプレイドライバ２９を省略した構成とすることもでき、その場合、アンテナを介してデータを送受信することによりＰＤＡや携帯電話にディスプレイ機能を持たせることが可能である。

【００６６】上記のように電源としてキャパシター３１又は二次電池を使用し、充電は接触型/非接触型ともに次のようにして行うことができる。すなわち、電池内蔵

ウォレットに装着した状態で充電しながらキー操作を行い電池内蔵ウォレットからＩＣカードを取り外す。また、電池内蔵ウォレットに装着して充電し、電池内蔵ウォレットからＩＣカードを取り外した状態でキー操作を行うようにしてもよい。また、店頭端末のリーダーライターに装着した時に充電してもよい。

【００６７】図４にＰＤＡや携帯電話とのインターフェースを有するＩＣカード１２の構成を示す。同図に示すように、図３に示す構成からテンキーとＬＣＤに関わる部分を除いた構成をとる。この場合、ＥＰＲＯＭ２５には、プログラムと秘密鍵と共に、携帯電話やＰＤＡの認証に用いる公開鍵を有する。また、ＰＤＡや携帯電話から操作時に電力を供給することが可能である。

【００６８】次に、本発明の第１の実施例における処理手順を図５を用いて説明する。

【００６９】まず、ＩＣカード所有者はテンキー付きＩＣカード、ディスプレイ/テンキー付きＩＣカード、又はＰＤＡ、携帯電話等を用いて、ＩＣカードにパスワードを入力する（ステップ１）。パスワードの表示は〝＊〟等の記号を用いるか〝Enter〟キー入力で消去される(ディスプレイなしのＩＣカードではこの制御は不要である。)。なお、パスワードや生体情報等の個人を証明するための情報を本明細書では個人情報という。

【００７０】次に、利用者はＩＣカードを店頭端末のリーダーライターに装着する（ステップ２）。なお、非接触型ＩＣカードを用いる場合は接近させるだけでよい。

【００７１】続いて、ＩＣカードは属性情報を認証センターに送る（ステップ３）。属性情報を受信した認証センターは認証信号をＩＣカードに送る（ステップ４）。この認証信号は認証の度に異なる値をとる。認証信号を受信したＩＣカードは一回のパスワード入力に対して一回のみ、認証信号とパスワードとを連結したデータに例えば秘密鍵による暗号化を施して認証応答信号を生成し、認証センターに送り返す（ステップ５）。上記の属性情報は例えばカードＩＤである。

【００７２】認証センターは認証応答信号を公開鍵で復号化し、認証センターが有する当該ＩＣカードの属性情報に対するパスワードと、復号化して得たパスワードとを比較して正しいことを確認すると、認証済信号を店頭端末に送り（ステップ６）、認証応答信号が正しくないことを確認すると認証拒否信号を店頭端末に送る（ステップ７）。

【００７３】上記の例の認証処理の場合、認証センターは図６に示すようなテーブルを有し、このテーブルに記録されたパスワードと、演算によって得たパスワードとの比較を行うことによってパスワード認証を行う。

【００７４】なお、上記のようにパスワードを用いず、認証センターから送信された認証信号を秘密鍵で暗号化して認証センターに送り返し、認証センターがそれを復号することでＩＣカード自体の認証を行うことは可能である。この場合のパスワードは、例えば、ＩＣカードを有効にするために使用できる。

【００７５】ＩＣカードが一回のパスワード入力に対して一回のみ認証を行うようにするには、例えば、図７に示す処理を行う。すなわち、パスワードを入力し（ステップ１０１）、上記の認証処理を行い（ステップ１０２）、認証処理が終了したらＩＣカード内のパスワードを削除する（ステップ１０３）。

【００７６】上記の説明ではパスワードを例にとって説明したが、指紋等の生体情報やその他の個人情報を認証に使用する場合にも同様に処理を行うことが可能である。

【００７７】さて、パスワード認証処理以降の処理は電子決済の方式により異なるので、それぞれについて分けて説明する。

【００７８】まず、クレジットカード型決済処理について説明する。

【００７９】ＩＣカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ１１）。次に、店頭端末は決済センター(クレジット会社)に取引額の支払を要求し（ステップ１２）、決済センター(クレジット会社)は決済日に所有者の銀行口座から要求額を引き落とし、取引先(加盟店)の口座に取引額から手数料を減算した金額を振り込む（ステップ１３）。

【００８０】次に、電子マネー型決済処理について説明する。

【００８１】上記と同様に、ＩＣカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ２１）。次に、店頭端末はＩＣカードの貨幣価値情報を取引額だけ減算し取引先(加盟店)の貨幣価値情報を加算し（ステップ２２）、決済センター(カード発行金融機関)に獲得した貨幣価値情報を送る（ステップ２３）。決済センター(カード発行金融機関)は取引先(加盟店)の口座に貨幣価値情報の金額を振り込む（ステップ２４）。なお、手数料がある場合はそれを減算した金額を振り込む。

【００８２】次に、キャッシュカード型決済処理について説明する。

【００８３】ＩＣカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ３１）。店頭端末は決済センター(カード発行金融機関)に取引額の支払を要求し（ステップ３２）、決済センター(カード発行金融機関)は所有者口座から要求額を引き落とし、取引先(加盟店)の口座にその金額を振り込む（ステップ３３）。なお、手数料がある場合はそれを減算した金額を振り込む。

【００８４】なお、上記の各決済センターは、各処理の履歴の管理・報告等も行う。

【００８５】［第２の実施例］次に、本発明の第２の実施例について、図８を用いて説明する。

【００８６】第２の実施例では、パスワードに加え、ＩＣカードに取引限度額を入力する。これにより、取引限度額を超える取引を防止することができ、安全に取引を行うことができる。

【００８７】まず、第１の実施例で説明したように、パスワードをＩＣカードに入力する（ステップ４１）。次に、ＩＣカードに取引限度額を入力する（ステップ４２）。

【００８８】続いて、ＩＣカードを店頭端末のリーダーライターに装着することによって、第１の実施例で説明したようなパスワード認証処理が行われる（ステップ４３）。

【００８９】これ以降の処理は電子決済の方式により異なるので、それぞれについて分けて説明する。

【００９０】まず、クレジットカード型決済処理について説明する。

【００９１】ＩＣカードは属性情報と取引限度額情報を決済センターに送る（ステップ５１）。ＩＣカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ５２）。なお、この処理は省略してもよい。そして、店頭端末は決済センター(クレジット会社)に取引額の支払を要求する（ステップ５３）。決済センター(クレジット会社)はＩＣカードの取引限度額を越えた取引先(加盟店)からの取引要求を拒絶する（ステップ５４）。取引限度額を超えていない場合には、決済センター(クレジット会社)は決済日に所有者の銀行口座から要求額を引き落とし、取引先(加盟店)の口座に取引額から手数料を減算した金額を振り込む（ステップ５５）。

【００９２】図９に、上記の決済センターの処理フローを示す。まず、取引限度額をＩＣカードから受信する（ステップ１１１）。その後、取引額を店頭端末から受信する（ステップ１１２）。そして、取引額と取引限度額とを比較し（ステップ１１３）、取引額が取引限度額以上であれば取引要求を拒絶し（ステップ１１４）、取引額が取引限度額より小さければ上述した口座処理を行う（ステップ１１５）。

【００９３】次に、電子マネー型決済処理について説明する。

【００９４】ＩＣカード所有者は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ６１）。なお、この処理は省略してもよい。次に、ＩＣカードは、店頭端末からＩＣカードの取引限度額を越える決済要求があるとき、その決済要求を拒絶する（ステップ６２）。

【００９５】店頭端末からの決済要求がＩＣカードの取引限度額を超えない場合には、店頭端末はＩＣカードの貨幣価値情報を取引額だけ減算し取引先(加盟店)の貨幣価値情報を加算する（ステップ６３）。続いて、店頭端末は決済センター(カード発行金融機関)に獲得した貨幣価値情報を送る（ステップ６４）。

【００９６】決済センター(カード発行金融機関)は取引先(加盟店)の口座に貨幣価値情報の金額を振り込む（ステップ６５）。なお、手数料がある場合はそれを減算した金額を振り込む。

【００９７】上記の電子マネー型の場合の取引限度額判断に係わるＩＣカードの処理フローを図１０に示す。まず、店頭端末から決済要求とともに取引額を受信する（ステップ１２１）。その取引額とユーザが入力した取引限度額とを比較し（ステップ１２２）、取引額が取引限度額以上であれば決済要求を拒絶し（ステップ１２３）、取引額が取引限度額より小さければＩＣカードの貨幣価値情報を取引額だけ減算する（ステップ１２４）。

【００９８】次に、キャッシュカード型決済処理について説明する。

【００９９】まず、ＩＣカードは属性情報と取引限度額情報を決済センターに送る（ステップ７１）。続いて、ＩＣカード所有者（ユーザ）は店頭端末で取引金額を確認し、正しければ確認ボタンを押す（ステップ７２）。なお、この処理は省略することが可能である。次に、店頭端末は決済センター(カード発行金融機関)に取引額の支払を要求する（ステップ７３）。要求を受けた決済センター(カード発行金融機関)はＩＣカードからの取引限度額を越えた取引先(加盟店)からの決済要求を拒絶する（ステップ７４）。

【０１００】決済要求がＩＣカードからの取引限度額を超えない場合には決済センター(カード発行金融機関)は所有者口座から要求額を引き落とし、取引先(加盟店)の口座に該金額を振り込む（ステップ７５）。なお、手数料がある場合はそれを減算した金額を振り込む。この場合の決済センターの処理フローは図９に示した処理フローと同様である。

【０１０１】第２の実施例において、支払額データをＩＣカードに書込み、必要に応じて表示することにより、取引限度額までいくらあるかを容易に把握することが可能となる。

【０１０２】［第３の実施例］次に、第３の実施例を図１１を用いて説明する。第３の実施例では、パスワードに加え、ＩＣカードに取引額を入力する。これにより、安全に取引を行うことができるとともに、金額確認の操作を省略することが可能である。以下、第１、第２の実施例と異なる部分を中心に説明する。

【０１０３】利用者は、店頭端末にＩＣカードを装着する前にＩＣカードに取引額を入力する（ステップ８１）。ここで、第３の実施例で使用するＩＣカードには、正確な取引額を入力するために消費税を加算するキーを設けるようにしてもよい。このキーには、ディスプレイ／テンキー付きＩＣカードを使用する方式ではボタンを使用し、ＰＤＡや携帯電話で情報をＩＣカードに入

力する方式ではボタンでもソフトスイッチでも使用可能である。このようなキーを用いて、購入した複数商品の総額や消費税の加算の計算を行い、ＩＣカードに正確な取引額を入力する。この後、ＩＣカードを店頭端末に装着し（ステップ８２）、パスワード認証（ステップ８３）が行われる。

【０１０４】クレジットカード型、キャッシュカード型の場合、パスワード認証の後にＩＣカードは属性情報と取引額情報を決済センターに送る（ステップ８４）。そして、店頭端末は決済センターに取引額の支払を要求する（ステップ８５）。なお、第３の実施例では取引額を利用者がＩＣカードに入力しているため、店頭端末による金額確認は行わない。

【０１０５】決済センターは、ＩＣカードから受信した取引額と異なる取引額の支払いを要求した取引先からの取引要求を拒絶する（ステップ８６）。ＩＣカードから受信した取引額と店頭端末からの取引額が一致した場合には、第１、２の実施例で説明した引き落とし、振り込み処理等の口座処理が行われる。

【０１０６】電子マネー型の場合、ＩＣカードは、ＩＣカードに入力された取引額と異なる決済要求が店頭端末からあるとき、その決済要求を拒絶する（ステップ９１）。店頭端末からの決済要求がＩＣカードの取引額と一致する場合には、第２の実施例で説明した電子マネー型決済処理におけるステップ６３以降と同様の決済処理が行われる。

【０１０７】上記の決済センターの処理フローを図１２に示す。まず、ＩＣカードから予め入力された取引額を受信する（ステップ１３１）。次に、店頭端末から取引要求とともに取引額を受信する（ステップ１３２）。これらの取引額を比較し（ステップ１３３）、一致しなければ取引要求を拒絶し（ステップ１３４）、一致する場合には口座処理を行う（ステップ１３５）。

【０１０８】次に、電子マネー型の場合の取引限度額判断に係わるＩＣカードの処理フローを図１３に示す。まず、店頭端末から決済要求とともに取引額を受信する（ステップ１４１）。その取引額とユーザが入力した取引額とを比較し（ステップ１４２）、それらが一致しなければ決済要求を拒絶し（ステップ１４３）、一致すればＩＣカードの貨幣価値情報を取引額だけ減算する（ステップ１４４）。

【０１０９】なお、第２と第３の実施例を組み合わせて、取引限度額と取引額をＩＣカードに入力するようにしてもよい。

【０１１０】本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【０１１１】

【発明の効果】本発明によれば、店頭端末にＩＣカードを装着する前にパスワードを入力するので、店頭端末の改造等によってパスワードを記録される危険を無くすことができる。また、店頭端末へのパスワード入力時間を削減し、利用者の利便性が向上するとともに、店における業務効率を向上させることができる。

【０１１２】パスワードに係るセキュリティーが向上することにより、クレジットカード型では、本人認証をサインからパスワードに代えることでき、事務経費の削減により手数料を低額にできるという効果がある。また、電子マネー型では、ＩＣカードの収納額を高額にすることができる。更に、キャッシュカード型では、パスワード(銀行口座暗証番号)が盗まれることの問題を解決できる。

【０１１３】また、取引限度額をＩＣカードに入力し、それを決済センターに送信等することとしたので、店頭端末の改造等による不正や本人の過誤による過大な額の取引を防止することが可能となる。

【０１１４】また、消費税を含めた取引額をＩＣカードに入力し、その額と店頭端末が算出した取引額とを比較し、一致した場合にのみ取引を行うこととしたため、店頭端末の改造等による不正な取引を防止することが可能となる。また、店頭端末への金額確認ボタンの操作が不要になるため、利用者の利便性が向上するとともに、店における業務効率を向上させることができる。特に、電子マネー型では小額取引が多いので、金額確認ボタン操作不要の効果は大きい。

【０１１５】上記のようにセキュアで利便性の高いな電子決済システムを提供することが可能になるので、当該電子決済システムの運営者はより多くのクライアントと加盟店を確保でき、より多くの取引に利用されることを期待することができる。

【０１１６】

【図面の簡単な説明】

【図１】電子決済システムの構成図である。

【図２】決済センターの構成図である。

【図３】ディスプレイとテンキー付きＩＣカードの構成図である。

【図４】ＰＤＡ等とのインターフェースを有するＩＣカードの構成図である。

【図５】本発明の第１の実施例における処理手順を示す図である。

【図６】認証センターが有するテーブルの例を示す図である。

【図７】ＩＣカードが一回のパスワード入力に対して一回のみ認証を行うようにするための処理を示すフローチャートである。

【図８】本発明の第２の実施例における処理手順を示す図である。

【図９】本発明の第２の実施例における決済センターの処理を示すフローチャートである。

【図１０】本発明の第２の実施例における電子マネー型

の場合のＩＣカードの処理を示すフローチャートである。

【図１１】本発明の第３の実施例における処理手順を示す図である。

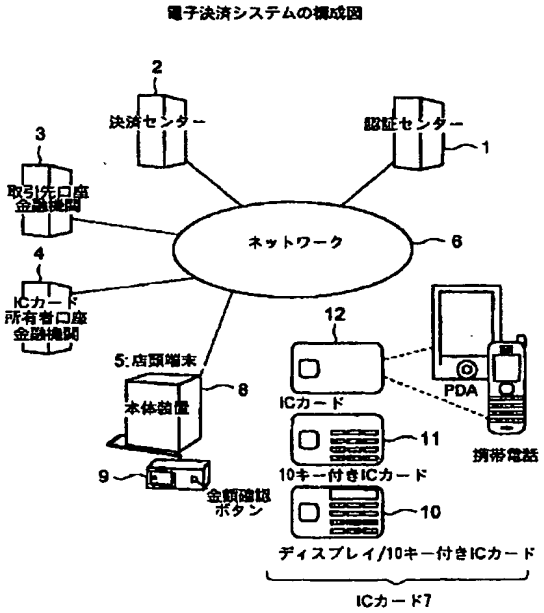
【図１２】本発明の第３の実施例における決済センターの処理を示すフローチャートである。

【図１３】本発明の第３の実施例における電子マネー型の場合のＩＣカードの処理を示すフローチャートである。

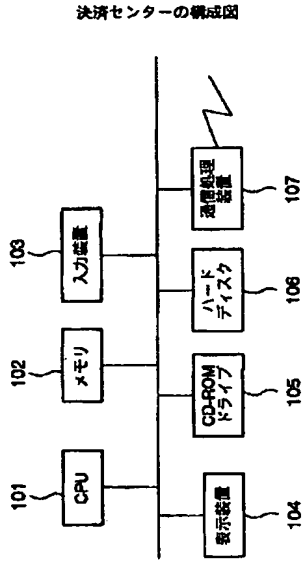
【符号の説明】

１　認証センター
２　決済センター
３　取引先口座金融機関
４　ＩＣカード所有者口座金融機関
５　店頭端末
６　ネットワーク
７　ＩＣカード
８　本体装置
９　リーダーライター
１０　ディスプレイとテンキー付きＩＣカード
１１　テンキー付きＩＣカード
１２　ＰＤＡや携帯電話とのインターフェースを有するＩＣカード
２１　アンテナ
２２　トランシーバ
２３　ＣＰＵ
２４　ＲＡＭ
２５　ＥＰＲＯＭ
２６　テンキー
２７　テンキーエンコーダ
２８　ＬＣＤ（liquid crystal display）
２９　ディスプレイドライバ
３０　受電器
３１　キャパシタ
３２　切替器３２
１０１　ＣＰＵ（中央処理装置）
１０２　メモリ
１０３　入力装置
１０４　表示装置
１０５　ＣＤ－ＲＯＭドライブ
１０６　ハードディスク
１０７　通信処理装置

【図１】

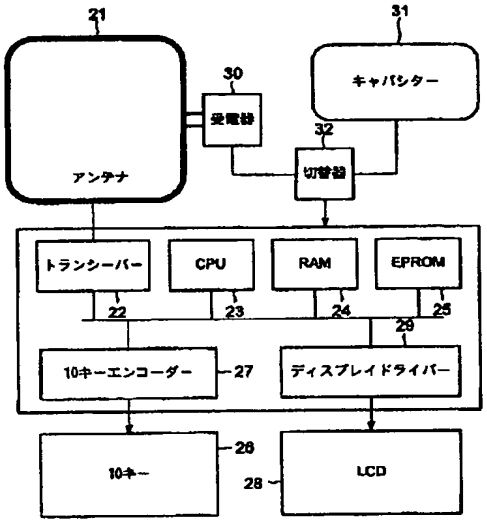


【図２】



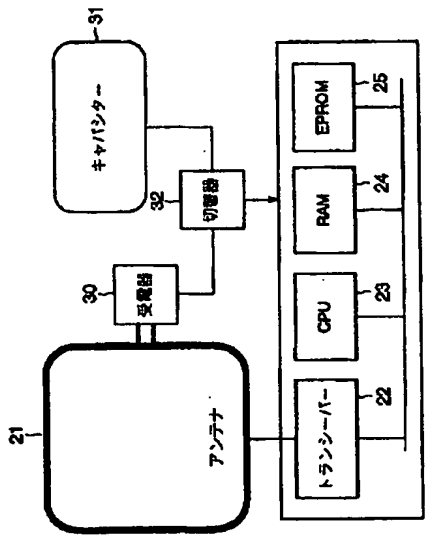
【図３】

ディスプレイとテンキー付きICカードの構成図



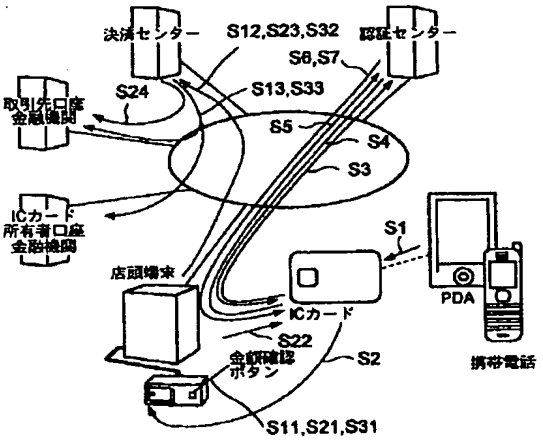
【図４】

PDA等とのインターフェースを有するICカードの構成図



【図５】

本発明の第1の実施例における処理手順を示す図



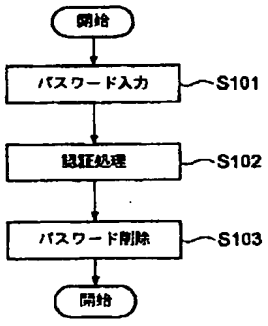
【図６】

認証センターが有するテーブルの例を示す図

属性情報	パスワード
abcd	× × × ×
efgh	△ △ △ △
・ ・ ・	・ ・ ・

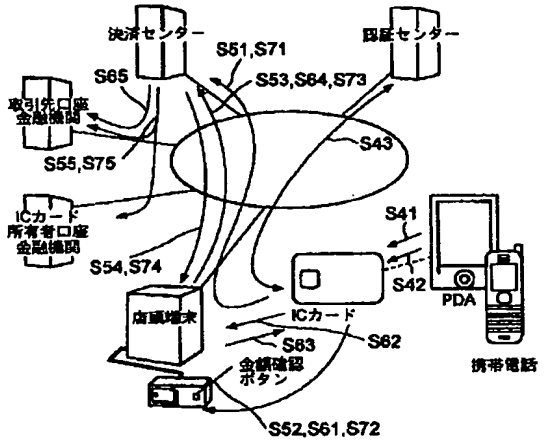
【図７】

ICカードが一回のパスワード入力に対して一回のみ認証を行うようにするための処理を示すフローチャート



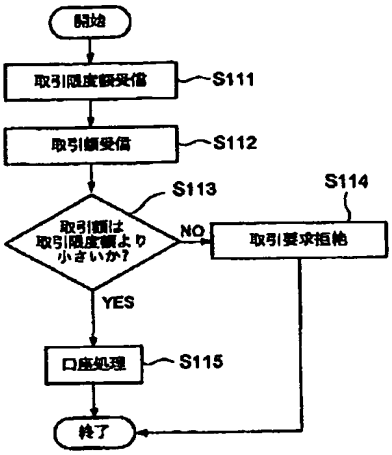
【図８】

本発明の第2の実施例における処理手順を示す図



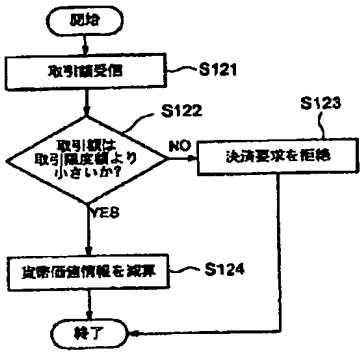
【図９】

本発明の第2の実施例における決済センターの処理を示すフローチャート



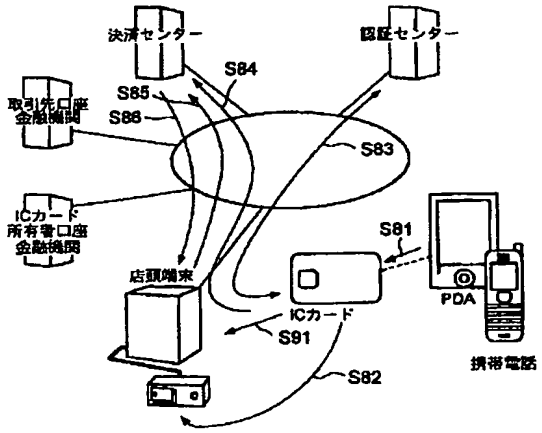
【図１０】

本発明の第2の実施例における電子マネー型の場合のICカードの処理を示すフローチャート



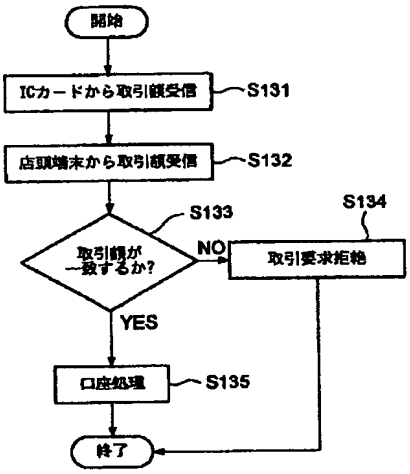
【図１１】

本発明の第3の実施例における処理手順を示す図



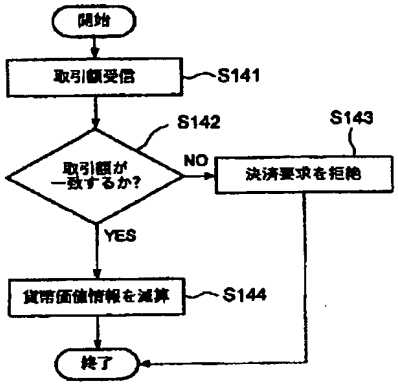
【図１２】

本発明の第3の実施例における決済センターの処理を示すフローチャート



【図１３】

本発明の第3の実施例における電子マネー型の場合のICカードの処理を示すフローチャート



フロントページの続き

(51) Int. Cl.[7]	識別記号	FI		テーマコード(参考)
G06K	17/00	G06K	17/00	V 5B085
	19/077		19/00	K
	19/07			J

Fターム(参考) 2C005 MA04 MA05 MA33 MB08 NA09
QA05 QB01 QC20 SA04 SA05
SA06 SA12 SA13 SA16 TA22
5B035 AA15 BB09 CA05 CA06
5B049 AA05 CC39 DD04 EE21 EE26
5B055 CB00 HA02 KK05 KK19
5B058 KA38 YA01
5B085 AA08 AE02 AE12